EXHIBIT A

MONROE COUNTY CLERK'S OFFICE

THIS IS NOT A BILL. THIS IS YOUR RECEIPT.

Receipt # 2552065

Book Page CIVIL

No. Pages: 24

Instrument: EFILING INDEX NUMBER

Control #: 202011181316
Index #: E2020009128

Date: 11/18/2020

Time: 4:48:24 PM

Return To:
CONOR THOMAS TALLET

LaPrairie, Eric

Presidio, Inc.
Presidio Holdings Inc.
Presidio LLC
Presidio Networked Solutions LLC
Presidio Networked Solutions Group, LLC

State Fee Index Number	$165.00
County Fee Index Number	$26.00
State Fee Cultural Education	$14.25
State Fee Records Management	$4.75
Total Fees Paid:	$210.00

Employee: MJ

State of New York

MONROE COUNTY CLERK'S OFFICE
WARNING – THIS SHEET CONSTITUTES THE CLERKS ENDORSEMENT, REQUIRED BY SECTION 317-a(5) & SECTION 319 OF THE REAL PROPERTY LAW OF THE STATE OF NEW YORK. DO NOT DETACH OR REMOVE.

JAMIE ROMEO

MONROE COUNTY CLERK

SUPREME COURT
STATE OF NEW YORK COUNTY OF MONROE

ERIC LAPRAIRIE, *on behalf of himself and all other employees similarly situated,*

Plaintiff,

v.

PRESIDIO, INC., PRESIDIO HOLDINGS INC., PRESIDIO LLC, PRESIDIO NETWORKED SOLUTIONS LLC, PRESIDIO NETWORKED SOLUTIONS GROUP, LLC, AND PRESIDIO TECHNOLOGY CAPITAL, LLC,

Defendants.

SUMMONS

Index No.

_____

Date Index No. Purchased:

November 18, 2020

TO THE ABOVE-NAMED DEFENDANTS:

YOU ARE HEREBY SUMMONED to answer the complaint in this action and to serve a copy of your answer or, if the complaint is not served with this summons, to serve a notice of appearance, on Plaintiff's attorneys within 20 days after the service of this summons, exclusive of the day of service, where service is made by delivery upon you personally within the state, or within 30 days after completion of service where service is made in any other manner. In case of your failure to appear or answer, judgment will be taken against you by default for the relief demanded in the complaint.

Plaintiff designates Monroe County as the place of trial. The basis of venue in this Court is that Defendants transact business within Monroe County.

Dated: November 18, 2020

THOMAS & SOLOMON LLP

By: _____

J. Nelson Thomas, Esq.
Jessica L. Lukasiewicz, Esq.
Jonathan W. Ferris, Esq.
Conor T. Tallet, Esq.
Attorneys for Plaintiff
693 East Avenue
Rochester, New York 14607
Telephone: (585) 272-0540
nthomas@theemploymentattorneys.com
jlukasiewicz@theemploymentattorneys.com
jferris@theemploymentattorneys.com
ctallet@theemploymentattorneys.com

SUPREME COURT
STATE OF NEW YORK COUNTY OF MONROE

ERIC LAPRAIRIE, *on behalf of himself and all other employees similarly situated,* *Plaintiff,* v. PRESIDIO, INC., PRESIDIO HOLDINGS INC., PRESIDIO LLC, PRESIDIO NETWORKED SOLUTIONS LLC, PRESIDIO NETWORKED SOLUTIONS GROUP, LLC, AND PRESIDIO TECHNOLOGY CAPITAL, LLC, *Defendants.*	CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL Index No. _____

Plaintiff Eric LaPrairie ("Named Plaintiff"), individually and on behalf of all other employees similarly situated (collectively "Plaintiffs" of the "Class Members"), by and through his attorneys, Thomas & Solomon LLP, brings this class action complaint against Presidio, Inc., Presidio Holdings Inc., Presidio LLC, Presidio Networked Solutions, LLC, Presidio Networked Solutions Group, LLC, and Presidio Technology Capital, LLC ("Presidio" or "Defendants"), and alleges as follows:

NATURE OF ACTION

1. Named Plaintiff brings this action on behalf of himself and all other employees similarly situated against Presidio as a result of Presidio's failure to adequately safeguard and protect the personally identifiable information ("PII") of their employees and by negligently disclosing such employee PII to cyber criminals.

2. Plaintiffs are all current or former employees of Defendants whose PII was compromised as a result of an unknown third-party gaining unauthorized access to Presidio's software and/or systems on or about March 5, 2020 (hereinafter the "Data Breach" or

"Breach").

3. The Breach resulted in the disclosure of Plaintiffs' private and sensitive PII, including their names, Social Security numbers, compensation and tax information.

4. For the rest of their lives, Named Plaintiff and Class Members will bear an immediate and heightened risk of all manners of identity theft.

5. Indeed, Plaintiffs have also suffered concrete harm almost immediately after the Data Breach. For example, Named Plaintiff himself fell victim to attempted identity theft just months after the Data Breach and was forced to spend numerous hours rectifying the harm caused by Defendants' conduct. Additionally, the unauthorized third party also altered direct deposits of some Class Members and wrongfully diverted such direct deposit funds.

6. Accordingly, Named Plaintiff brings this action as a direct and/or proximate result of the Data Breach. Plaintiffs have incurred, and will continue to incur, damages in the form of, among other things, attempted identity theft, time and expense in mitigating harms caused by Defendants' conduct, increased risk of harm, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

JURISDICTION AND VENUE

7. The jurisdiction of this Court is invoked pursuant to the CPLR §§ 301 and 302 because Defendants transact and/or solicit business within the state from which they derive substantial revenues and because this action arises from Defendants' activities in New York.

8. Venue is appropriate in this Court since Defendants conduct business within Monroe County.

THE PARTIES

Named Plaintiff

9. Named Plaintiff Eric LaPrairie is a resident of Michigan and a former employee of Presidio.

10. Named Plaintiff worked for Presidio from approximately January 2019 to August 2019 and he received a notice on or around April 26, 2020 from Presidio informing him that his PII had been disclosed in a data breach.

Defendants

11. Defendant Presidio, Inc. is a Delaware corporation with its principal place of business in New York.

12. Defendant Presidio Holdings Inc. is a Delaware corporation with its principal place of business in New York.

13. Defendant Presidio LLC is a Georgia limited liability company with its principal place of business in New York.

14. Defendant Presidio Networked Solutions LLC is a Florida limited liability company with its principal place of business in New York.

15. Defendant Presidio Networked Solutions Group, LLC is a Delaware limited liability company with its principal place of business in New York.

16. Defendant Presidio Technology Capital, LLC is a Georgia limited liability company with its principal place of business in New York.

17. Together, Defendants conduct business within Monroe County.

18. For example, Presidio has employees and actively recruits new employees in Rochester, New York for its growing Western, New York sales team.

FACTS

19. As a condition of Plaintiffs' employment, Plaintiffs provided their PII to Defendants in order to verify their identities, receive compensation, and for Defendants to maintain complete employee records for, among other things, tax purposes.

20. On or about March 5, 2020, an unauthorized third-party gained access to Defendants' servers and systems resulting in the Data Breach and subsequent exposure of PII of thousands of current and former employees of Presidio.

21. In approximately late April 2020, over a month after the Breach, Plaintiffs received correspondence from Defendants informing them of the circumstances of the Breach.

22. The correspondence also informed Plaintiffs that their PII was compromised in the Breach, including their name, Social Security number, compensation and tax information.

23. Being in the cybersecurity industry, Presidio knew or should have known of the importance of safeguarding employee PII, as well as the consequences of the unauthorized disclosure of employees' PII. Defendants, however, failed to implement adequate policies and procedures to safeguard Plaintiffs' PII from being disclosed by hackers and cyber criminals.

24. Despite being aware of their common law and statutory duty to adequately safeguard Plaintiffs' PII, Defendants breached that duty by disclosing Plaintiffs' PII through their negligent actions and/or inactions.

25. Defendants negligently failed to take the necessary precautions required to safeguard and protect Plaintiffs' PII from unauthorized disclosure. Defendants' actions and/or inactions amount to a flagrant disregard of Plaintiffs' rights to privacy and property.

26. Defendants' actions and/or inactions caused Plaintiffs to suffer injury and damages as described herein.

27. As a result, Defendants are liable to Named Plaintiff and Class Members as described herein.

28. Additionally, Defendants are liable under the statutes, laws, and regulations of each state in which they operate throughout the United States.

Personally Identifiable Information (PII)

29. PII "refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as data and place of birth, mother's maiden name, etc." *See* Office of Mgmt. & Budget, Memorandum M-07-16, *Safeguarding Against & Responding to the Breach of Personally Identifiable Information*, at n.1 (May 22, 2007), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

30. PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners that cause great harm to the individuals who have had their PII exposed.

31. The PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. For example, personal information can be sold at prices ranging from $40 to $200. *See* Anita George, *Your Personal Data is for Sale on the Dark Web. Here's How Much it Costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

32. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," and that is "as good as your DNA to hackers." *See*

Cameron Huddleston, *How to Protect Your Kids from the Anthem Data Breach*, Kiplinger (Feb. 10, 2015), https://www.kiplinger.com/article/credit/t048-c011-s001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

33. In the event of a compromised Social Security number, an individual must wait until she becomes a victim of identity theft before she can obtain a new one. Even then, the Social Security Administration warns "that a new number probably won't solve all [] problems . . . [and] won't guarantee [] a fresh start." *See* Soc. Sec. Admin., *Identity Theft and Your Social Security Number*, at 6 (June 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf. In fact, "[f]or some victims of identity theft, a new number actually creates new problems." *Id.* For example, a brand new Social Security number will have a completely blank credit history, making it difficult for an identity theft victim to get extended credit for years unless it is linked to the old compromised number.

34. Given the Data Breach at issue resulted in an unauthorized third-party gaining access to Plaintiffs' PII, it is reasonably foreseeable that cyber criminals can and will use the compromised PII in a variety of different unlawful ways to the detriment of Plaintiffs.

Defendants Were Aware of the Risk of Cyberattacks

35. In today's world, data security breaches are becoming increasingly common. So common that the Federal Trade Commission ("FTC") has issued an abundance of guidance for business to combat the ever-increasing threat to employees' PII. *See, e.g.*, FTC, *Data Breach Response: A Guide for Business* (May 2019), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf; FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.bulkorder.ftc.gov/publications/protecting-personal-information-guide-business;

FTC, *Start with Security: A Guide for Business* (Jun. 2015), https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf.

36. Given Presidio's position as a "leading North American IT solutions provider focused on . . . Cloud [and] Security & Emerging solutions[,]" Presidio was certainly aware of the risk of data breaches. To be sure, the front page of Presidio's website currently highlights October as "Cybersecurity Awareness Month" and offers assistance to its customers to "help *accelerate* required annual Cybersecurity *compliance* and *testing* initiatives." (emphasis in original).

37. Indeed, according to Presidio's 10-K annual report for the fiscal year ending June 30, 2019, Presidio identifies "cyber risk management, infrastructure security and managed security solutions" as one of its core business offerings. Presidio goes on to note that its cyber "[s]ecurity revenue increased $44.6 million, or 15.9%, . . . driven by higher demand from customers as they look to stay ahead of increasingly complex cyber security threats[.]"

38. In the same annual filing, Presidio identified "[d]isruptions or breaches of security in our information technology systems and the misappropriation of our clients' data could impair our reputation, expose us to liability and adversely impact our business" as a risk factor to its business.

39. As such, Presidio was well aware of the risk that data security breaches by "hackers and cyberterrorists . . . could [] expose [Presidio] to legal claims, investigations, proceedings and liability and to regulatory penalties under laws that protect the privacy of personal information[.]"

40. Thus, being in the cyber security field themselves, Defendants clearly knew or should have known of the risk of data breaches and should have maintained adequate safeguards for their own employees' PII.

41. Additionally, beyond their common law duty of care to adequately safeguard employees' PII, Defendants also had a statutory duty of care under New York Labor Law ("NYLL") § 203-d to implement policies or procedures to safeguard against a disclosure of employees' PII, which Defendants failed to implement despite its awareness of the potential threat.

Named Plaintiff and Class Members Have Suffered Concrete Injuries

42. Named Plaintiff and Class Members were obligated to provide Defendants with sensitive personal information.

43. As a direct and/or proximate result of Defendants' failure to adequately safeguard Plaintiffs' PII, Plaintiffs have or will suffer actual concrete injuries.

44. These actual injuries include out of pocket expenses and the value of their time reasonable incurred to remedy or mitigate the effect of the Data Breach relating to:

- Closely reviewing and monitoring bank accounts and credit reports;
- Purchasing credit monitoring and identity theft prevention;
- Addressing their inability to withdraw funds linked to compromised accounts;
- Placing "freezes" and "alerts" with credit reporting agencies;
- Contacting financial institutions and closing or modifying financial accounts.

45. Further, some Plaintiffs have already suffered concrete harm in the form of altered and wrongfully diverted direct deposit funds immediately following the Data Breach.

46. Additionally, Named Plaintiff himself suffered concrete harm in the form of attempted identity theft shortly after the Data Breach.

47. Specifically, in approximately May 2020, Named Plaintiff was victim to a "SIM swap" attack where a third-party used Named Plaintiff's PII to enter a T-Mobile store and swap

Named Plaintiff's telephone number over to the third-party's mobile phone. This allowed the unauthorized third-party to obtain Named Plaintiff's telephone number for unlawful use and access Named Plaintiff's email account he used for a variety of different online accounts.

48. With access to Named Plaintiff's telephone number and email, the third-party was able to reset Named Plaintiff's online account passwords in an effort to gain unauthorized access to Named Plaintiff's online accounts, including financial accounts, his Drop Box account housing his personal documents, and his Microsoft account.

49. After becoming aware of this identity attack, Named Plaintiff spent approximately 15-20 hours contacting T-Mobile support and fraud services, researching how to better protect his personal information from fraudulent intruders, implementing heightened security measures on his device and accounts to protect against fraudsters, and rectifying the harm caused by the identity attack. As a result, Named Plaintiff suffered harm in the form of lost time and invasion of privacy as a direct and/or proximate cause of Defendants' actions and/or inactions giving rise to the Data Breach.

50. Named Plaintiff not only suffered a concrete harm as described above, but will also continue to suffer an imminent and continuing injury of heightened risk of identity theft and/or unauthorized use of his PII.

51. Named Plaintiff and Class Members will forever be subject to an increased risk that cyber criminals will use their PII as a result of Defendants' failure to adequately safeguard Plaintiffs' PII. As a result, Named Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, time and out-of-pocket expenses in mitigating harms caused by Defendants' conduct, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

52. As a direct and/or proximate result of Defendants' failure to adequately safeguard Plaintiffs' PII, Plaintiffs have been deprived of the value of their PII, for which there is a well-established national and international market.

53. Defendants' actions have further placed Plaintiffs at an imminent, immediate, and continuing risk of identity theft and identity fraud. There is also a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported by Plaintiffs.

Defendants Response to the Data Breach is Inadequate to Protect the Plaintiffs

54. Despite failing to adequately safeguard Plaintiffs' PII, Defendants have failed to provide adequate compensation to the Plaintiffs harmed by their negligent acts and/or omissions.

55. Defendants have offered Plaintiffs just twelve (12) months, and only in some cases twenty-four (24) months, of credit monitoring service through *my*TrueIdentity. Even if a Plaintiff signs up for *my*TrueIdentity service, it will not provide Plaintiffs any compensation for the costs and burdens associated with fraudulent activity resulting from the Data Breach that took place prior to Plaintiffs signing up for the offered services. This is especially concerning where some Plaintiffs were not informed that their PII was compromised until over a month following the Breach.

56. Additionally, given the fact that Plaintiffs face a lifetime of increased risk of identity theft, twelve or twenty-four months of protection is wholly inadequate to compensate Plaintiffs for Defendants' wrongful conduct.

CLASS ACTION ALLEGATIONS

57. This action is maintainable as a class action under Article 9 of the CPLR.

58. The CPLR Article 9 class consists of:

> All persons, whether current or former employees or otherwise, whose PII was compromised as a result of the Data Breach that occurred on or about March 5, 2020.

59. Numerosity is satisfied as the Class size is believed to be over 40 members. For example, Presidio disclosed that 3,324 current and former employees were victim of the Data Breach. Thus, the Class is so numerous that joinder of all Class Members is impracticable.

60. Common issues of law and fact exist as to all Class Members and predominate over any questions affecting only individual Class Members. Among the common issues of law and fact are the following:

- Whether Defendants owed the Plaintiffs a duty to safeguard their PII;
- Whether Defendants breached that duty;
- Whether Defendants disclosed Plaintiffs' PII;
- Whether Plaintiffs have sustained monetary loss, and the proper measure of that loss;
- Whether Plaintiffs' damages were foreseeable; and
- Whether Defendants are liable for all damages claimed.

61. Named Plaintiff's claims are typical of the Class Members' claims because Named Plaintiff asserts claims against Defendants flowing from a single data security breach that occurred on or about March 5, 2020. Conversely, Defendants engaged in a unitary course of conduct that forms the basis of this lawsuit. Named Plaintiff is advancing the same claims and legal theories on behalf of himself and all Class Members.

62. Further, Named Plaintiff has no interest antagonistic to the Class, and has retained Thomas & Solomon LLP ("Class Counsel") as counsel.

63. Class Counsel is qualified and able to litigate Named Plaintiff's and Class Members' claims.

64. Class Counsel concentrates its practice in litigation, and its attorneys are experienced in class action litigation.

65. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and avoids duplication by allowing these claims to be prosecuted in a single action. Named Plaintiff and Class Members lack the resources to adequately prosecute separate claims, and the amounts that each individual stand to recover makes individual cases impractical to pursue. Further, the costs for the court system for adjudication of individualized litigation would be substantial. The only practical chance for Class Members to recover their illegally retained gratuities and wages is through a class action.

66. Defendants' wrongful actions, inaction, and omissions are generally applicable to the Class as a whole and therefore, Plaintiffs also seek equitable remedies for the Class.

67. Defendants' systemic policies and practices regarding the protection of PII also make injunctive relief for the Class appropriate.

FIRST CAUSE OF ACTION
Negligence

68. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

69. As a condition of their employment, Named Plaintiff and Class Members were obligated to provide Defendants with their PII.

70. As a sophisticated company with particular expertise in cyber security, Defendants had full knowledge of the sensitivity of their employees' PII, as well as the types

of harm Named Plaintiff and Class Members would suffer if their PII were to be exposed to cyber criminals.

71. Defendants owed a common law duty to Named Plaintiff and Class Members to exercise reasonable care in adequately safeguarding and protecting Named Plaintiff's and Class Members' PII in Defendants' possession.

72. Defendants assumed a duty of care to use reasonable means to secure and safeguard Named Plaintiff's and Class Members' PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of their servers or systems holding the PII.

73. Defendants breached their duty of care by failing to adequately secure and safeguard Named Plaintiff's and Class Members' PII by negligently storing and/or maintaining their servers and systems holding the PII.

74. Named Plaintiff and Class Members have suffered harm as a result of Defendant's' negligence.

75. Named Plaintiff not only suffered a concrete harm in the form of lost time and an invasion of privacy from the Data Breach as described above, but will also continue to suffer an imminent and continuing injury of heightened risk of identity theft and/or unauthorized use of his PII.

76. Named Plaintiff and Class Members will forever be subject to an increased risk that cyber criminals will use their PII as a result of Defendants' failure to adequately safeguard their PII. As a result, Named Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, time and expense in mitigating harms caused by Defendants' conduct, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

77. It was reasonably foreseeable that Defendants' failure to adequately safeguard Named Plaintiff and Class Members' PII would result in a cyber security breach and unauthorized disclosure of their PII by third-parties who would use and/or disseminate such PII for no lawful purpose.

78. Defendants as much as admit such foreseeability in their annual 10-K report identifying "[d]isruptions or breaches of security in our information technology systems and the misappropriation of our clients' data could impair our reputation, expose us to liability and adversely impact our business" as a risk factor to its business. As such, Presidio was well aware of the risk that security breaches by "hackers and cyberterrorists . . . could [] expose [Presidio] to legal claims, investigations, proceedings and liability and to regulatory penalties under laws that protect the privacy of personal information[.]"

79. But for Defendants' negligent and wrongful breach of their duty of care owed to Named Plaintiff and Class Members, their PII would not have been compromised.

80. As a direct and/or proximate result of Defendants' negligent conduct, the Data Breach resulted in an unauthorized disclosure of Named Plaintiff and Class Members' PII. As such, Named Plaintiff and Class Members have incurred (and will continue to incur) the above-referenced damages and injury.

81. Plaintiffs are also entitled to injunctive relief as well as actual and punitive damages.

82. Accordingly, Named Plaintiff and Class Members respectfully request that this Court award all relevant damages for Defendants' negligent failure to adequately safeguard PII.

SECOND CAUSE OF ACTION
Negligence Per Se

83. Named Plaintiff and Class Members re-allege the above paragraphs as if fully

restated herein.

84. NYLL § 203-d sets forth a statutory duty of care for employers with respect to the safeguarding of employee PII.

85. Specifically, the statute makes it illegal to "[c]ommunicate an employee's personal identifying information to the general public." *Id.* at § 203-d(1)(d).

86. The statute defines "personal identifying information" as a "social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number." *Id.*

87. The statute further articulates that "[i]t shall be presumptive evidence that a violation of this section was knowing if the employer has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." *See id.*

88. Defendants breached their statutory duty of care with respect to their handling of Named Plaintiff and Class Members' PII because Defendants' acts and/or omissions were unlawful violations of NYLL § 203-d. Specifically, Defendants failed to put in place sufficient policies or procedures to adequately safeguard Named Plaintiffs' and Class Members PII.

89. Named Plaintiff and Class Members are current or former employees of Defendants, which places them within the class of persons NYLL § 203-d is designed to protect.

90. As a result of Defendants' failure to implement such policies and procedures, the resulting Data Breach exposed Named Plaintiff's and Class Members' PII, resulting in damages in the form of among other things, attempted identity theft, time and expense in mitigating harms caused by Defendants' conduct, increased risk of harm, diminished value of their PII,

loss of privacy, and/or additional damages as set forth herein.

91. Named Plaintiff and Class Members have suffered and will continue to suffer damages and injuries as described herein.

92. Accordingly, Named Plaintiff and Class Members respectfully request that this Court award all relevant damages for Defendants' *per se* negligent failure to adequately safeguard PII.

THIRD CAUSE OF ACTION
Breach of Express Contract

93. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

94. Plaintiffs had written employment agreements with Defendants. The employment agreements involved a mutual exchange of consideration whereby Defendants entrusted Plaintiff and Class Members with particular job duties and responsibilities in furtherance of Defendants' services, in exchange for the promise of employment, with salary, benefits, and secure PII.

95. Defendants' failure to protect Plaintiffs' PII constitutes a material breach of the terms of the agreement by Defendants.

96. As a direct and proximate result of Defendants' breach of contract with Plaintiffs, Plaintiffs have been irreparably harmed.

97. Accordingly, Plaintiffs respectfully request this Court to award all relevant damages for Defendants' breach of express contract.

FOURTH CAUSE OF ACTION
Breach of Implied Contract

98. Named Plaintiff and Class Members re-allege the above paragraphs as if fully

restated herein.

99. Named Plaintiff and Class Members provided their PII in connection with their employment with Defendants in order to verify their identity, receive compensation, and for Defendants to have complete employee records for, among other things, tax purposes.

100. Named Plaintiff and the Class Members provided various sensitive PII to Defendants as a condition precedent to their employment with Defendants, or in connection with employer sponsored benefits.

101. Understanding the sensitive nature of Named Plaintiff's and Class Members' PII, Defendants implicitly promised Named Plaintiff and Class Members that they would adequately safeguard their sensitive and personal information, which was a material term of this contract.

102. Named Plaintiff and Class Members reasonably relied upon this covenant.

103. Further, Named Plaintiff and Class Members would not have disclosed their PII without such assurances from Defendants that such PII would be adequately safeguarded.

104. Despite implicitly promising to adequately safeguard the PII, Defendants materially breached their promise and failed to adequately safeguard Named Plaintiff and Class Members' PII.

105. As a direct and/or proximate result of Defendants' material breach, Named Plaintiff and Class Members have incurred (and will continue to incur) the above-referenced damages and injury.

106. Accordingly, Named Plaintiff and Class Members respectfully request that this Court award all relevant damages for Defendants' breach of implied contract.

FIFTH CAUSE OF ACTION
Unjust Enrichment

107. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

108. Defendants, by way of its affirmative actions and/or omissions, knowingly and deliberately enriched themselves by saving the costs it reasonably and contractually should have expended on adequate data security measures to maintain Named Plaintiff's and Class Members' PII.

109. Nevertheless, Defendants continued to obtain the benefits conferred on it by Named Plaintiff and Class Members, mainly from the labor contracted to in the employment agreements between the parties.

110. As a direct and proximate result of Defendants' decision to profit rather than provide adequate security measures to safeguard Named Plaintiff and Class Members' PII, Plaintiffs suffered and continue to suffer considerable injuries in the form of, among other things, attempted identity theft, time and expense in mitigating harms caused by Defendants' conduct, increased risk of harm, diminished value of their PII, loss of privacy, and/or additional damages as set forth herein.

111. Accordingly, Named Plaintiff and Class Members respectfully request this Court award relief in the form of restitution and/or compensatory damages.

SIXTH CAUSE OF ACTION
New York Labor Law § 203-d

112. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

113. Pursuant to New York Law, "[a]n employer shall not unless otherwise required

by law . . . (c) [p]lace a social security number in files with unrestricted access; or (d) [c]ommunicate an employee's personal identifying information to the general public." NYLL § 203-d(1)(c), (d).

114. The statute defines "personal identifying information" as a "social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to marriage, or drivers' license number." *See id.* at § 203-d(1)(d).

115. A violation of the statute provides for "a civil penalty of up to five hundred dollars on any employer for any knowing violation of this section." *See id.* at § 203-d(3). *See also Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739, 752 (S.D.N.Y. 2017) (holding NYLL "§ 203-d implies a private right of action").

116. The statute further articulates that "[i]t shall be presumptive evidence that a violation of this section was knowing if the employer has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." *See id.*

117. Defendants' acts and/or omissions were unlawful violations of NYLL § 203-d because Defendants had failed to put in place sufficient policies or procedures to adequately safeguard Named Plaintiffs' and Class Members PII—a risk in which Defendants were well aware.

118. As a result of Defendants' failure to implement such policies and procedures, the resulting Data Breach ensued exposing Named Plaintiff and Class Members to damages and injuries as described herein.

119. Accordingly, Named Plaintiff and Class Members respectfully request this Court

award statutory damages, compensatory damages, and injunctive relief for Defendants' knowing violations of NYLL § 203-d.

SEVENTH CAUSE OF ACTION
Violation of the Applicable State Laws

120. Named Plaintiff and Class Members re-allege the above paragraphs as if fully restated herein.

121. As a direct an proximate result of Defendants' actions and/or omissions described herein, and the resulting Data Breach exposing Named Plaintiff and Class Members' PII, Defendants are in violation of the following state laws similarly designed to protect Named Plaintiff and Class Members from the unauthorized disclosure of their PII:

- Cal. Bus. & Prof. Code §§ 17200, *et seq.*;
- Cal. Civ. Code §§ 1798.80, *et seq.*;
- 815 Ill. Comp. Stat. §§ 505/10a(a), 530/1, *et seq.*; and
- Md. Code, Com. Law §§ 13-408, 14-3501, *et seq.*

WHEREFORE, Named Plaintiff and the Class demand judgment against Defendants in their favor and that they be given the following relief:

(a) an order certifying the Class as requested and designating Thomas & Solomon LLP as class counsel;

(b) designation of Named Plaintiff Eric LaPrairie as the representative of the Class;

(c) holding that Defendants breached their duty to safeguard and protect Named Plaintiff's and Class Members' PII;

(d) awarding Named Plaintiff and Class Members appropriate relief, including actual, compensatory, statutory, punitive, and any other such damages as permitted by law;

(e) awarding equitable, injunctive, and declaratory relief as appropriate, including an Order requiring Defendants to immediately secure and fully encrypt all confidential information, to properly secure computers containing PII, to crease negligently storing, handling, and securing Plaintiffs' PII, and to provide additional years of identity theft monitoring;

(f) awarding reasonable attorneys' fees, expenses, expert fees, and costs incurred in vindicating Named Plaintiff's and Class Members' rights;

(g) an award of pre- and post-judgment interest;

(h) awarding a service payment for Named Plaintiff Eric LaPrairie; and

(i) such other and further legal or equitable relief as this Court deems just and appropriate.

JURY DEMAND

Pursuant to the CPLR, Plaintiff demands a trial by jury on all questions of fact.

Dated: November 18, 2020

THOMAS & SOLOMON LLP

By: _____

J. Nelson Thomas, Esq.
Jessica L. Lukasiewicz, Esq.
Jonathan W. Ferris, Esq.
Conor T. Tallet, Esq.
Attorneys for Plaintiff
693 East Avenue
Rochester, New York 14607
Telephone: (585) 272-0540
nthomas@theemploymentattorneys.com
jlukasiewicz@theemploymentattorneys.com
jferris@theemploymentattorneys.com
ctallet@theemploymentattorneys.com